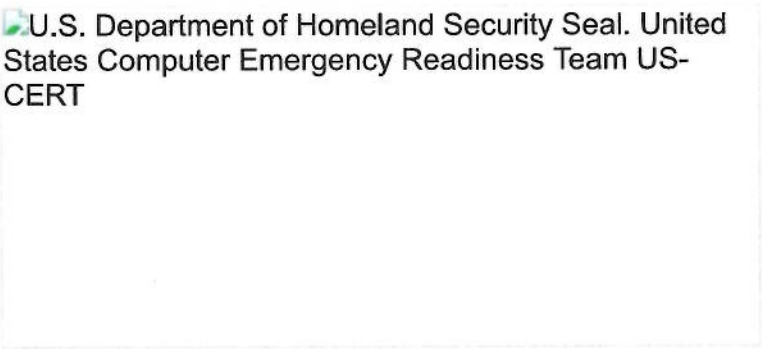
EXHIBIT G



Advisory (ICSA-17-124-01)

Hikvision Cameras

Original release date: May 04, 2017

CVSS v3 10.0

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Hikvision

Equipment: Cameras

Vulnerabilities: Improper Authentication, Password in Configuration File

AFFECTED PRODUCTS

Hikvision reports that the following cameras and versions are affected:

- DS-2CD2xx2F-I Series
  - V5.2.0 build 140721 to V5.4.0 build 160530
- DS-2CD2xx0F-I Series
  - V5.2.0 build 140721 to V5.4.0 Build 160401
- DS-2CD2xx2FWD Series
  - V5.3.1 build 150410 to V5.4.4 Build 161125
- DS- 2CD4x2xFWD Series
  - V5.2.0 build 140721 to V5.4.0 Build 160414
- DS-2CD4xx5 Series
  - V5.2.0 build 140721 to V5.4.0 Build 160421
- DS-2DFx Series
  - V5.2.0 build 140805 to V5.4.5 Build 160928
- DS-2CD63xx Series
  - V5.0.9 build 140305 to V5.3.5 Build 160106

IMPACT

Successful exploitation of these vulnerabilities could lead to a malicious attacker escalating his or her privileges or assuming the identity of an authenticated user and obtaining sensitive data.

MITIGATION

Hikvision has released updates to mitigate the improper authentication vulnerability in cameras sold through authorized distributers. Hikvision has not mitigated the password in configuration file vulnerability.

However, Hikvision is aware of so-called "grey market" cameras which are sold via unauthorized channels. These cameras often use unauthorized firmware created by sources outside of Hikvision. In the case of these "grey market" devices, updating the firmware may result in converting the camera's interface back to its original state. Users of "grey market" cameras who cannot update due to this unauthorized firmware will still be susceptible to these vulnerabilities.

In the Hikvision Unauthorized Distributors Notice, Hikvision encourages users to use devices sold by authorized distributers rather than so-called "grey market" devices. Hikvision's Unauthorized Distributors Notice can be found at the following location:

http://www.hikvision.com/us/about.aspx?stat=1&c_kind=293&c_kind2=10631

North American models of Hikvision cameras which can be fixed and their updated firmware versions are listed below:

- DS-2CD2xx2F-I Series
  - V5.4.5 build 170123 and later
- DS-2CD2xx0F-I Series
  - V5.4.5 Build 170123 and later
- DS-2CD2xx2FWD Series
  - V5.4.5 Build 170124 and later
- DS- 2CD4x2xFWD Series
  - V5.4.5 Build 170228 and later
- DS-2CD4xx5 Series
  - V5.4.5 Build 170302 and later
- DS-2DFx Series
  - V5.4.9 Build 170123 and later
- DS-2CD63xx Series
  - V5.4.5 Build 170206 and later

These updates are available for download at the following location:

http://www.hikvision.com/us/about_10805.html

More information can be found by visiting Hikvision's Vulnerability Notice:

http://www.hikvision.com/us/about_10807.html

For Chinese-language domestic cameras, Hikvision also provides on-site tours or remote support in addition to the updated firmware listed above.

Hikvision also states that device models and firmware upgrade procedures may differ between regions. These policies will be communicated to users through Hikvision.

NCCIC/ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploits specifically target these vulnerabilities.

VULNERABILITY OVERVIEW

IMPROPER AUTHENTICATION CWE-287

The improper authentication vulnerability occurs when an application does not adequately or correctly authenticate users. This may allow a malicious user to escalate his or her privileges on the system and gain access to sensitive information.

CVE-2017-7921 has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

PASSWORD IN CONFIGURATION FILE CWE-260

The password in configuration file vulnerability could allow a malicious user to escalate privileges or assume the identity of another user and access sensitive information.

CVE-2017-7923 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

RESEARCHER

IPcamtalk user "Montecrypto" identified these vulnerabilities.

BACKGROUND

Critical Infrastructure Sector(s): Critical Manufacturing and others

Countries/Areas Deployed: Worldwide

Company Headquarters Location: China

Contact Information

For any questions related to this report, please contact the NCCIC at:

Email: NCCICCUSTOMERSERVICE@hq.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: http://ics-cert.us-cert.gov
or incident reporting: https://ics-cert.us-cert.gov/Report-Incident?

The NCCIC continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.